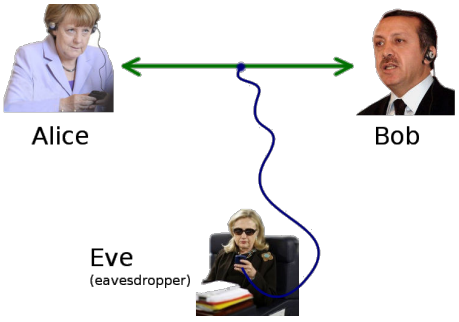

Cryptography [Didia, Wikimedia]

Exercise 7.1: Quantum Cryptography (8P)

Encrypted communication requires that both parties share a key (a random sequence of classical bits) that can be used to encode and decode messages by bitwise XOR operations. The problem of encryption therefore reduces to safely generate identical keys on both sides. In 1992 H.C. Bennett proposed a particularly simple protocol (B92):

> Alice randomly generates a classical bit $a \in \{0,1\}$, using it to prepare a qubit
>
> $$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a = 0 \\ |+\rangle & \text{if } a = 1 \end{cases}$$
>
> where $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$. Then she sends this qubit to Bob.
>
> Likewise Bob randomly generates a classical bit $b \in \{0,1\}$. He uses this bit to select one of the two measurement apparatuses
>
> $$\mathbf{M}_0 = |0\rangle\langle 0| - |1\rangle\langle 1|\,, \qquad \mathbf{M}_1 = |+\rangle\langle +| - |-\rangle\langle -|$$
>
> which is then used to measure Alice's incoming qubit. Then he sends the measurement result $m = \pm 1$ by classical public communication to Alice. Both Alice and Bob repeat the process until they get the result $m = -1$.

(a) Show that $a = 1 - b$ if $m = -1$, that is, the locally generated bits are opposite. (2P)

(b) How many qubits are on average needed to generate a bit of the key? (1P)

(c) Suppose that Eve intercepts the communication in that she measures the transferred qubit by a projective measurement $\mathbf{E} = |\phi_+\rangle\langle\phi_+| - |\phi_-\rangle\langle\phi_-|$, where

$$|\phi_+\rangle = \alpha|0\rangle + \beta|1\rangle\,, \qquad |\phi_-\rangle = \beta^*|0\rangle - \alpha^*|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1$$

are two arbitrary orthogonal states. Show that Eve's interception generally changes the measurement statistics seen from the perspective of Bob and Alice, depending effectively on two parameters $u := |\alpha|^2$ and $v := \frac{1}{2}|\alpha + \beta|^2$. (3P)

(d) Determine u and v such that Bob and Alice cannot detect the interception. (1P)

Please turn over ⇒

(e) In the case of (d), is it possible for Eve to get information about the key? (1P)

Exercise 7.2: Supremum norm of operators (4P)

The supremum norm of a bounded operator $\mathbf{M}$ is defined by

$$||\mathbf{M}|| = \sup_{|\psi\rangle} \frac{||\,\mathbf{M}|\psi\rangle\,||}{||\,|\psi\rangle||\,},$$

where $||\,|\psi\rangle|| = \langle\psi|\psi\rangle$ is the usual vector norm in the Hilbert space.

(a) Show that $||\mathbf{M}||$ is the square root of the maximal eigenvalue of $\mathbf{M}^\dagger\mathbf{M}$. (2P)

(b) Prove that the norm $||\mathbf{M}||$ is subadditive $\big(||\mathbf{M}+\mathbf{N}|| \leq ||\mathbf{M}|| + ||\mathbf{N}||\big)$ and submultiplicative $\big(||\mathbf{MN}|| \leq ||\mathbf{M}||\,||\mathbf{N}||\big)$. (2P)

(Σ = 12P)

To be handed in on Monday, December 11, at the beginning of the tutorial.